La Revue des droits de l'homme
Revue du Centre de recherches et d'études sur les droits fondamentaux
Actualités Droits-Libertés | 2017

L'État de surveillance au régime sec : la CJUE renforce la prohibition de la surveillance "de masse"

Droit à la vie privée (CJUE)

Jean-Philippe Foegle

OpenEdition Journals

Édition électronique
URL : http://journals.openedition.org/revdh/2966
DOI : 10.4000/revdh.2966
ISSN : 2264-119X

Éditeur
Centre de recherches et d'études sur les droits fondamentaux

Référence électronique
Jean-Philippe Foegle, « L'État de surveillance au régime sec : la CJUE renforce la prohibition de la surveillance "de masse" », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 08 février 2017, consulté le 19 avril 2019. URL : http://journals.openedition.org/revdh/2966 ; DOI : 10.4000/revdh.2966

L'État de surveillance au régime sec : la CJUE renforce la prohibition de la surveillance "de masse"

Droit à la vie privée (CJUE)

Jean-Philippe Foegle

1 « *Si désirez être bon Pantagruélistes (c'est à dire vivre en paix, joie, santé, faisant toujours grande chère), ne vous fiez jamais aux gens qui regardent par un pertuis* ».

2 A l'instar du héros rabelaisien Pantagruel, l'état de surveillance est un glouton d'informations : là où les régimes démocratiques accordent aux citoyens un large droit à détenir des informations sur les activités des gouvernements tout en respectant une sphère d'intimité à l'abri de leurs incursions, les régimes de surveillance tendent à maintenir le secret sur leurs activités tout en contraignant des citoyens à révéler à leur insu des aspects toujours plus importants de leur vie privée[1]. Dans l'Union Européenne toutefois, à l'heure où une forme de « patriotisme constitutionnel européen » tend à conduire la Cour de Justice de l'Union Européenne à renforcer le rôle des droits fondamentaux de l'Union dans la constitutionnalisation des valeurs démocratiques et en particulier de la valeur vie privée[2] le développement d'un état de surveillance trouve sa limite dans la double émergence du droit à la protection des données personnelles, et dans la transparence imposée aux Etats via le développement des fuites lancées par des lanceurs d'alerte[3]. Complexe et encore constitué de clairs obscurs, l'état actuel de la jurisprudence tracée par les cours de Strasbourg et de Luxembourg en matière de vie privée est le résultat direct des révélations d'Edward Snowden et des controverses transatlantiques suscitées par celles-ci.

3 Dès 2013, ces révélations suscitent en effet une dénonciation sans ambiguïtés de la surveillance de masse aussi bien dans le cadre de l'Union européenne[4] que du Conseil de l'Europe[5] ou encore de l'ONU[6]. Mais celle-ci conduit toutefois, paradoxalement, à ancrer les exigences de sécurité dans un discours fondé sur les droits fondamentaux : la condamnation de la surveillance de masse s'était, comme dans l'arrêt Klass contre Allemagne[7], opéré au prix d'une légitimation de la surveillance en démocratie. Enfermé

dans une stratégie de dénégation et dans une tentative d'esquiver les aspects les plus polémiques du débat, le gouvernement américain a néanmoins entamé un début de retraite stratégique en procédant à la publication rapide d'un rapport - « Liberty and Security in a changing world » - reprenant des critiques déjà formulées de longue date[8] contre les excès rendus possibles par le « Patriot Act ».

4 Dans un second temps, cette controverse a donné lieu à des décisions de juridictions suprêmes – à l'exception du Conseil constitutionnel français – visant à renforcer les droits fondamentaux dans ce domaine. En Europe, après la retentissante décision Digital Rights Ireland de 2014[9], nombre de juridictions nationales ont procédé à une invalidation des lois sur la surveillance électronique sur le fondement de la Charte des droits fondamentaux, notamment au Royaume-Uni[10]. Aux États-Unis, l'invalidation de l'article 215 de la FISA pour des motifs purement techniques avait préparé la réforme en demi-teinte du Patriot Act par le Freedom Act[11]. Toutefois, sous couvert de favoriser les libertés, celui-ci conforte en réalité l'arsenal de surveillance dont disposent les agences nord-américaines de renseignement[12].

5 Dans un troisième temps, la Cour de justice a invalidé la décision 2000/520/CE relative aux transferts de données à caractère personnel vers les États-Unis, fondant la prohibition de la surveillance de masse sur une double garantie liée au droit à la vie privée et à la protection des données personnelles[13] et au droit au recours effectif. L'analyse de la décision en lien avec les arrêts Zakharov et Szabo[14] ayant procédé à une condamnation similaire de la surveillance tous azimuts permet de constater que le principe même de la surveillance « de masse » est sévèrement condamné en droit européen des droits de l'Homme. Une telle émergence d'un socle de droits intangible à la vie privée devrait logiquement inciter les États-Unis à changer leur législation, confortant ainsi le statut de l'Union Européenne en tant qu'« exportateur de normes »[15]. Mais celle-ci avait évidemment un effet interne d'avoir des incidences sur les lois votées par les Parlements nationaux en matière de surveillance secrète dans l'Union Européenne.

6 C'est précisément dans la continuité de cette « troisième étape » des controverses transatlantiques relatives à la vie privée que le présent arrêt s'inscrit, confirmant la solution édictée dans les arrêts Schrems et Digital Rights de la CJUE d'une part, et des arrêts Zakharov et Szabo de la CEDH d'autre part.

7 L'affaire avait trait à l'application de la directive « vie privée et communications électroniques », dite directive « e-privacy »[16] lue à la lumière des droits consacrés par la Charte des Droits Fondamentaux. Celle-ci, qui prévoit un principe général de confidentialité des communications électroniques, permet néanmoins en son article 15 aux États de prendre des mesures pour poursuivre des objectifs d'intérêt général, en particulier tels que la lutte contre le terrorisme et la criminalité grave. Cette dérogation ouvre dans ces hypothèses aux État le droit de demander aux fournisseurs d'accès internet de conserver les métadonnées de leurs clients.

8 Or, avant l'arrêt Digital Rights, nombre de législation nationales avaient mis en place, en transposition de la directive, une telle conservation de données, donnant lieu à de très nombreux contentieux. Restait alors à savoir si, évacuée par la Cour, une telle possibilité pouvait être réintroduite via l'article 15 de la directive e-privacy, qui prévoit la possibilité de déroger dans certaines hypothèses au principe de confidentialité des communications électroniques.

9 Les deux questions préjudicielles soumises à la Cour concernaient précisément la compatibilité de telles législations au droit de l'Union et à la Charte. Étaient en cause la législation suédoise et la législation du Royaume-Uni, qui prévoyaient un mécanisme de conservation des données en tous points similaires à la directive de 2006. Légitimement saisies d'un doute sur la conformité au droit de l'Union de telles dispositions, les juridictions de renvoi ont sursis à statuer et posé trois questions distinctes relatives à l'interprétation de la Charte des Droits Fondamentaux de l'Union.

10 La première question d'importance, posée par la juridiction britannique, concernait le fait de savoir si l'arrêt Digital Rights avait bel et bien établi des exigences impératives en droit de l'Union, applicables au régime d'un État membre régissant l'accès aux données conservées. Une telle question se justifiait, aux yeux de la juridiction de renvoi, par le fait que la Cour ne s'était prononcée que sur les dispositions de la directive et non celles d'une réglementation nationale. Surtout, aux yeux de la juridiction de renvoi, la CJUE aurait, dans l'arrêt Digital Rights, uniquement examiné la légalité du régime de conservation des données par les opérateurs de télécommunications et n'aurait donc pas envisagé d'énoncer des exigences s'appliquant au droit interne encadrant l'accès à ces mêmes données par les États-membres. Ces derniers auraient donc toute latitude pour requérir des opérateurs de télécommunication qu'ils leur communiquent les données qu'ils possèdent sur leurs clients.

11 La seconde concernait plus directement la compatibilité au regard de l'article 15 – et donc de la charte de l'Union- d'une obligation générale de conservation de données, relative à toute personne et à tous les moyens de communication électronique et portant sur l'ensemble des données relatives au trafic, sans qu'aucune différenciation, limitation ni exception soit opérée en fonction de l'objectif de lutte contre la criminalité.

12 Enfin, la dernière question, posée par la juridiction suédoise, concernait les garanties à mettre en place pour permettre de rendre une telle législation compatible aux exigences énoncées dans l'arrêt Digital Rights s'agissant notamment s'agissant de l'encadrement des modalités d'accès aux données, des exigences de sécurité des données collectées par les fournisseurs d'accès, et de la durée de conservation admissible de ces données.

13 Invalidant les législations en cause, la Cour de justice confirme l'application des garanties issues de l'arrêt Digital Rights Ireland aux législations nationales, confirmant par la même occasion la prohibition de principe de la surveillance dite "de masse" ou, plus exactement, le fait que celle-ci présente un caractère indifférencié et susceptible de s'appliquer à tous les citoyens sans distinction (1°). Elle saisit surtout l'occasion pour préciser pour la première fois les exigences devant présenter une législation relative à l'accès des autorités publiques dans le prolongement des arrêts Zakharov et Szabo de la Cour de Strasbourg (2°).

1°/- Une prohibition réaffirmée de la collecte "en masse" des métadonnées

14 Ayant conclu à l'applicabilité de la Charte des droits fondamentaux, la Cour se livre, comme dans son arrêt Schrems, à une application « large » des considérants de l'arrêt Digital Rights Ireland, qu'elle vient compléter et renforcer. La prohibition de la surveillance de masse apparaît ainsi doublement fondée sur le droit à la protection des données personnelles, mais également sur la liberté d'expression. En effet, les juges de

Luxembourg soulignent explicitement que la protection contre la surveillance massive participe du respect de l'article 11 de la Charte garantissant le droit à la liberté d'expression. En effet une telle législation nationale est de nature à de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante[17] et, par conséquent, d'avoir un effet dissuasif sur l'usage par ceux-ci de leur liberté d'expression.

15 A ce titre, la Cour rappelle que la collecte des métadonnées, qui ne permet pas aux autorités d'accéder au contenu des communications, si elle ne porte pas atteinte au contenu même du droit à la vie privée, a des incidences sur la vie privée car des conclusions très précises sur celle-ci peut être tirée à partie des données conservées[18]. Il est notamment possible de retrouver et d'identifier la source d'une communication et la destination de celle-ci, de déterminer la date, l'heure, la durée et le type de communication, le matériel utilisé, ainsi que de localiser un appareil mobile. Or, ces données permettent un profilage précis des individus[19] (arrêt commenté, §98). Par conséquent, au vu de l'ampleur de l'atteinte à la vie privée et – indirectement – à la liberté d'expression qui en découle, une telle collecte non seulement doit être limitée à la lutte contre la criminalité grave[20], mais même dans ces hypothèses ne pas prévoir une conservation généralisée et indifférenciée de l'ensemble des données de connexion (arrêt commenté, §§102 et 103). En clair, la collecte doit être ciblée : un lien de stricte nécessité doit exister entre la quantité et l'ampleur des catégories de données collectées d'une part, et la lutte contre la criminalité d'autre part.

16 Or, d'une part, cette collecte concerne en l'espèce l'ensemble des utilisateurs de services de communications électroniques, y compris des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien avec des infractions pénales graves, et des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel[21] (arrêt commenté, §105). D'autre part, la réglementation en cause ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et n'est pas limitée à une période temporelle et / ou une zone géographique ou à un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave (arrêt commenté, §106). Celle-ci peut donc en théorie s'appliquer à l'ensemble des citoyens, y compris à ceux envers lequel il n'y a aucune suspicion de préparation ou de participation à un acte de terrorisme ou de criminalité grave.

17 Par suite, les législations en cause dépassent le strict caractère de précision, de nécessité et de proportionnalité que doivent revêtir des atteintes au droit à la vie privée et à la protection des données personnelles. En outre, dans un obiter dictum, la Cour précise, à toutes fins utiles au sujet de ces lois, dans le prolongement de l'arrêt Digital Rights qu'une telle législation devrait indiquer en quelles circonstances et sous quelles conditions – c'est à dire dans quelles hypothèses – une mesure de conservation des données peut être prise. Il s'agit de limiter celle-ci au strict nécessaire au vu des objectifs légitimes poursuivis.

18 Puis, s'agissant de la quantité de données collectées, la loi doit établir un rapport entre les données à conserver et l'objectif poursuivi, qui doivent clairement délimiter l'ampleur d'une telle collecte, en limitant les catégories de données collectées au strict nécessaire. Enfin, une telle législation doit être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec la criminalité grave (arrêt commenté, §§108-111). De manière novatrice, la Cour précise

qu'une telle délimitation peut être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe dans de telles zones un risque élevé de préparation ou de commission de tels actes.

19 Toutefois, cette réintroduction d'un critère excessivement large – le critère géographique - permettant de justifier des collectes « en masse » des données, démontre que ce n'est pas tant le principe de collecte massive de données qui est en cause, que l'absence de différenciation et de critères permettant de prévoir précisément les hypothèses dans lesquelles il est légitime de s'attendre à faire l'objet d'une telle collecte. La Cour semble utiliser ici le standard d'« aspiration raisonnable à la vie privée » utilisé par la Cour dans de nombreuses hypothèses depuis l'arrêt Halford c. Royaume-Uni de 1997[22], qui implique que les individus puissent prévoir dans quelles hypothèses ils peuvent faire l'objet d'une surveillance. Il s'agit d'éviter que la suspicion d'une surveillance généralisée n'en vienne à saper les fondements de la démocratie en ayant un effet dissuasif sur la liberté d'expression.

20 Une telle interprétation est au demeurant confirmée par le fait que l'arrêt rappelle que « l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête » (arrêt commenté, §103)[23], ce qui fait écho au considérant 69 de la décision Szabo.

*

2°/- Une surveillance secrète à visage humain ? Le "mode d'emploi" du droit européen des droits de l'Homme.

21 Mettant explicitement en œuvre non seulement l'arrêt Digital Rights, mais également expressément les arrêts Zakharov et Szabo de la Cour de Strasbourg, la Cour de justice précise pour la première fois les exigences devant présenter une législation relative à la surveillance des communications concernant l'accès aux données, leur durée de conservation ainsi que leur protection et conditions de sécurité. La jurisprudence de la Cour européenne et celle de la Cour de justice constituent donc l'avers et le revers de la même médaille : celle d'une condamnation ferme de la surveillance tous azimuts. En conséquence, il n'est pas inutile de rappeler les fondements des arrêts Zakharov et Szabo pour cerner avec précision les contours de cette ferme prohibition.

22 Dans l'arrêt Zakharov, la Cour avait fait grief à une législation nationale de ne pas avoir énoncé avec suffisamment de précision les circonstances dans lesquelles les pouvoirs publics sont habilités à recourir aux mesures de surveillance. Elle avait notamment souligné que la législation russe de ne donnait aucune indication sur « les circonstances dans lesquelles les communications d'une personne peuvent être interceptées en raison de faits ou d'activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique [...] », ce qui conférait aux autorités une « latitude quasi illimitée » en la matière[24]. Si l'arrêt Zakharov ne concernait stricto-sensu que des mesures de surveillance ciblées et ne portait pas sur le cas spécifique de l'interception de toutes les données à tout moment, celui-ci condamnait a fortiori ce type de surveillance, comme en témoigne

l'affaire Szabo. Dans ce dernier arrêt, la Cour avait noté que la législation hongroise « peut potentiellement affecter tout le monde et, qu'à ce titre, elle peut être interprétée comme ouvrant la voie à la surveillance illimitée d'un grand nombre de citoyens »[25].

23 Dans l'arrêt du 21 décembre 2016, la Cour de Luxembourg fait, à son tour, une application fidèle de cette jurisprudence. Rappelant qu'une réglementation nationale doit non seulement limiter l'accès aux données détenues par des fournisseurs de télécommunications aux infractions graves, mais également prévoir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées, celle-ci précise qu'un accès aux données ne peut être accordé qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Les seules exceptions possibles sont les hypothèses où des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme et que l'accès aux données d'autres personnes permettre de faire face à la menace. Dans ce cas, encore faut-il qu'il existe des éléments objectifs permettant de considérer que ces données pourraient être utiles à l'objectif de combattre un tel péril (arrêt commenté, §§115-118).

24 S'agissant du contrôle de telles mesures, les juges du plateau de Kirchberg précisent que - sauf cas d'urgence -, celles-ci doivent faire l'objet d'un contrôle a priori en étant subordonné effectué soit par une juridiction soit par une entité administrative indépendante. La décision de cette juridiction ou entité doit intervenir à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales (arrêt commenté, §125). En tout état de cause, une telle autorité doit présenter des garanties d'indépendance à défaut de quoi les personnes dont les données à caractère personnel ont été conservées seraient privées du droit à faire rectifier ou effacer leurs données (arrêt commenté, §120). En outre, ces mesures doivent préserver la possibilité d'un contrôle a posteriori de ces mesures en informant les personnes concernées de l'existence d'une collecte dès le moment où cette information n'est pas susceptible de compromettre les enquêtes menées par ces autorités (arrêt commenté, §121).

25 Une telle prise de position apparaît conforme à la "nouvelle" approche en la matière ne saurait être mieux résumée que par l'opinion concordante du juge bulgare dans l'arrêt Zakharov. Celui-ci estimait que l'appréciation large de la condition de victime pourrait servir à « une amélioration de la législation en matière de mesures opérationnelles d'investigation et à l'établissement d'un système effectif de contrôle public sur la surveillance »[26].

26 Si la CJUE ne précise pas la nature des garanties d'indépendance que devraient présenter les autorités indépendantes charger du contrôle a posteriori et a priori des mesures de conservation et accès aux données, l'arrêt Zakharov permet une fois de plus d'éclairer les zones d'ombres de l'arrêt de la Cour. Dans ce jugement, les juges du palais des droits de l'homme avaient précisé qu'il importe que l'organisme de contrôle soit suffisamment indépendant à l'égard de l'exécutif et dispose de tous les pouvoirs nécessaires s'assurer que l'interception des données présente un caractère de nécessité et de proportionnalité au regard des buts poursuivis « en vérifiant par exemple s'il est possible d'atteindre les buts recherchés par des moyens moins restrictifs »[27]. En outre, les pouvoirs de l'organe de contrôle relativement aux infractions qu'il peut déceler, constituent « un aspect important pour l'appréciation de l'effectivité du contrôle qu'il exerce »[28].

27 Soulignons sur ce dernier point qu'il résulte tant de la jurisprudence de la CJUE que de celle de la CEDH[29] que l'autorité juridictionnelle saisie d'une demande relative à la protection des droits d'une personne doit avoir accès à toutes les informations utiles à la résolution du litige, y compris des informations classées secret défense, étant entendu désormais que les juges internes doivent avoir le pouvoir, si nécessaire au regard du principe du contradictoire et de l'issue du litige, déclassifier des informations indûment classées secrètes et les verser au débat[30].

28 Enfin, les personnes privées chargées de conserver les données doivent assurer la pleine intégrité et la confidentialité desdites données, garantir un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles appropriées. En particulier, la réglementation nationale doit prévoir la conservation sur le territoire de l'Union ainsi que la destruction irrémédiable des données au terme de la durée de conservation de celles-ci.

29 Si la Cour ne s'aventure pas sur le terrain de la définition d'une durée acceptable de conservation des données, l'approche devant être adoptée en la matière se déduit du point 242 des conclusions de l'avocat général qui, citant l'arrêt Digital Rights, estime que les juridictions doivent déterminer si les données conservées peuvent être distinguées en fonction de leur utilité et si la durée de conservation a été adaptée en fonction de ce critère. Ces mêmes juridictions doivent vérifier que la durée de conservation est fondée sur des critères objectifs permettant de garantir que celle-ci est limitée au strict nécessaire

*

Conclusion

30 Le présent jugement "boucle la boucle" en matière de surveillance des données personnelles des citoyens de l'Union. Confirmant la triple opposabilité des garanties de l'article 8 aux institutions de l'Union européenne (Digital Rights), aux transferts de données vers l'étranger (Schrems) et aux Etats-membres eux-mêmes (arrêt commenté), celui-ci aura des incidences nombreuses non seulement sur les législations des Etats-membres, mais également sur la future -et déjà contestée- directive européenne relative à la lutte contre le terrorisme.

31 Cette condamnation ad libitum de la surveillance électronique de masse confirme une fois de plus la fonction de charnière des droits à la vie privée et à la protection des données personnelles, ces droits servant non seulement à une interpénétration croissance des ordres juridiques de la Convention européenne et du droit de l'Union européenne en matière de vie privée, mais également à la circulation entre les deux ordres de solutions normatives s'étendant au droit au recours effectif et à la liberté d'expression. En cela, la constitutionnalisation du droit de l'Union contribue au rayonnement d'une politique "démocratique" de l'information[31] - à savoir une limitation de l'opacité entourant les activités gouvernementales doublée d'une limitation des catégories d'informations sur la vie privée des citoyens que peuvent obtenir les pouvoirs publics. Les deux ordres juridiques s'intègrent tous deux dans ce que l'avocat général Kokott décrivait comme une exigence plus large de transparence et de prévisibilité des traitements de données personnelles[32], explicitement liée au droit au recours effectif. L'important désormais n'est

plus tant de protéger une sphère d'intimité que de garantir la loyauté des violations de la vie privée en permettant aux individus de prévoir "raisonnablement" les hypothèses dans lesquelles leur vie privée sera violée, et d'exercer un recours contre les intrusions illicites dans leur vie privée

32 Cette « procéduralisation » de la vie privée conduit paradoxalement à affaiblir la notion même de vie privée au sens de l'article 8 de la Convention européenne au profit d'un droit à la protection personnelle dont les garanties sont essentiellement procédurales, et non substantielles. Le présent jugement est topique à cet égard : faisant référence à la jurisprudence de Strasbourg pour édicter les garanties procédurales devant être respectées dans la mise en oeuvre d'une surveillance numérique, la Cour se montre d'autant plus souple sur l'admission du principe de la violation de la vie privée des individus pour lutter contre la menace terroriste, en soulignant qu'une collecte de grandes quantités de données peut être justifiée dans certaines hypothèses limitatives à condition que ladite collecte ne soit pas indifférenciée.

33 Or, ce développement d'obligations procédurales positives – garantir la transparence des traitements de données et l'accès à un recours effectif – au détriment de l'obligation négative – plus classique – de ne pas intervenir dans une sphère d'intimité bien délimitée des individus fait courir le risque d'une perte de sens du droit à la vie privée. Pour reprendre une distinction introduite par Robert Post, le droit à la vie privée "classique" et le droit à la protection des données personnelles relèvent de deux logiques peu conciliables : là où le premier relève d'une logique communautaire (community) consistant à définir collectivement le niveau d'autonomie acceptable des individus dans une société démocratique politiquement constituée, le second relève d'une logique managériale ne visant qu'à encadrer de manière optimale l'usage d'informations personnelles par des bureaucraties privées et publiques, sans que la légitimité du principe d'un tel usage ne soit en question.

34 Ainsi "avalées" par le droit à la protection des données personnelles, les protections de la vie privée insaturées dans le cadre de l'article 8 de la convention perdent de leur clarté et, à minima de leur fonction promotionnelle[33] encourageant de manière diffuse le respect de la vie privée-intimité, ce qui fait courir le risque d'entraîner les juridictions dans une pente glissante[34]. Le risque ici est d'admettre, au nom de la "lutte contre le terrorisme", des atteintes de plus en plus larges à l'intimité des personnes au motif de l'existence de garanties procédurales adéquate.

35 Ainsi, le développement d'un droit fondamental autonome à la protection des données personnelles pourrait conduire à admettre le développement de la surveillance comme un phénomène inéluctable, instrumentalisant la valeur "vie privée" en faveur d'une nouvelle gouvernance de l'information.

36 Voilà qui ne serait pas le moindre des paradoxes à l'heure où le déploiement d'une crise de l'idéal des droits de l'homme fait mourir l'ancien monde sans que ne puisse encore advenir le nouveau[35].

*

37 **CJUE, Grande Chambre, 21 décembre 2016, *Tele2 Sverige AB et Secretary of State for the Home Department*, Aff. C-203/15 et C-698/15**

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner et se désabonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Jack Balkin, "The constitution in the national surveillance state", *Minnesota Law Review*, 2008, vol. 93, no 1.

2. V. sur ce paradigme : Paul De Hert, Serge Gutwirth. "Data protection in the case law of Strasbourg and Luxemburg : Constitutionalisation in action." (2009) : 3-44.

3. Vigjilenca Abazi, "Leaked Transparency and Whistleblowers", *VerfBlog,* 2 mai 2016.

4. V., du côté du Parlement Européen, la Résolution P7_TA-PROV(2014)0230 du 12 mars 2014 *sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures* du 2 mars 2014 ; et plus récemment, les études du Parlement Européen sur les risques et opportunités suscités par les mutations numériques et l'émergence de la surveillance de Masse : « Mass surveillance, part II – Technology foresight, options for longer term security and privacy improvements » ; « Mass surveillance, part I – Risks and opportunities raised by the current generation of network and applications »,, décembre 2014.

5. V., publié quelques mois après les révélations Snowden : Arcadio Diaz Terera, « La sécurité nationale et l'accès à l'information », Conseil de l'Europe, CDCJ(2013)13293, Strasbourg, Septembre 2013 ; et, plus récemment, Peter Omtizgt, « Les opérations massives de surveillance en Europe », Conseil de l'Europe, CDCJ(2014), AS/Jur(2015)01, Strasboug, janvier 2015.

6. Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression, A/HRC/23/40 , 2013.

7. Cour EDH, 6 septembre 1978, Klass et autres c/ Allemagne, n° 5029/71

8. V. Lisa Nelson, " Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era" *Public Administration Review*, 2004, vol. 64, no 3, p. 259-269; Paul Jaeger, John Carlo Bertot, Charles R Mclure, "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act" *Government Information Quarterly*, 2003, vol. 20, no 3, p. 295-314.

9. CJUE [GC], 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., aff j. C-293/12 & C-594/12. V. Florence Benoit-Rohmer, « Protection des données personnelles », *RTDE* 2015, p. 168 ; Denys Simon, « La révolution numérique du juge de l'Union : les premiers pas de la cybercitoyenneté », *Europe* n° 7, p. 4 ; Marie-Laure Basilien-Gainche, « Une prohibition européenne claire de la surveillance électronique de masse », in *Revue des droits de l'homme*, 14 mai 2014.

10. UK High Court, "David Davis and others -v- Secretary of State for the Home Department"*., 17 juillet 2015*

11. H.R. 2048, Pub.L. 114–23.

12. V. *Spencer Ackerman, 17 April 2015).* "Weakened surveillance reform bill is 'yesterday's news', civil libertarians say". *The Guardian, 17 avril 2015 ; Stephanie Condon,* "NSA surveillance reform bill now law"*, CBS News, 2 juin 2015 ;*

13. CJUE, Gr.Ch., 6 octobre 2015, Maximilian Schrems c. Data Protection Commissioner, aff. C-362/14 ; Jean-Philippe Foegle, « Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse », *La Revue des droits de l'homme* [En ligne], *Actualités Droits-Libertés*, mis en ligne le 30 mars 2016.

14. Jean-Philippe Foegle, « Chronique du droit « Post-Snowden »..., art. préc.

15. V. Sur cette notion : Zaki Laïdi. *La norme sans la force : l'énigme de la puissance européenne*, Presses de Sciences Po, 2014.

16. Yves Poullet, "About the E-Privacy Directive: towards a third generation of data protection legislation?", in *Data protection in a profiled world,* Springer Netherlands, 2010. p. 3-30.

17. CJUE, GC, 8 avril 2014, *Digital Rights Ireland Ltd , préc.*, §37.

18. La Cour cite en exemple les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées.

19. Ces données permettent d'après la Cour « *de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée* » (§96)

20. CJUE, GC , 8 avril 2014, *Digital Rights Ireland Ltd* , préc., §60.

21. *Ibid.*, §§57-58.

22. Cour EDH, 25 juin 1997, Halford c. Royaume-Uni, n° 20605/92.

23. V. aussi en ce sens les points 203 et 204 des conclusions de l'avocat général.

24. Cour. EDH, GC., 4 décembre 2015, Zakharov c. Russie, n° 47143/06, §248.

25. V. en ce sens: Sarah St. Vincent, "Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe "?, *CDT Blog,* 13 janvier 2016.

26. Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, Opinion concordante du Juge Dedov

27. Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, *préc.*, §260.

28. *Ibid*, §282.

29. CJUE 4 juin 2013, Z. Z., aff. C-300/11. V. Plus généralement, pour un aperçu des règles procédurales en Europe : Didier Bigo, Sergio Carrera, Nicholas Hernanz et Amandine Scherrer, National Security and Secret Evidence in Legislation and before the Courts : Exploring the Challenges, CEPS Paper in Liberty and Security in Europe No. 78, janvier 2015

30. Cour EDH, 2e Sect., 8 janvier 2013, Bucur et Toma c. Roumanie, n° 40238/02. §102.

31. Voir: Jack Balkin, "The first amendment is an information policy" *Hofstra Law Review*, 2013, vol. 41

32. V. conclusions de l'avocat général Juliane Kokott, 18 juillet 2007, *Promusicae contre contre Telefónica de España SAU*, aff. C-275/06, §53.

33. Voir, sur cette notion : Noberto Bobbio, *Essais de théorie du droit*, Bruylant-LGDJ, 1998, pp. 65 et suiv.

34. Voir, sur cette notion de slippery slope dans le cadre de la liberté d'expression : Eugene Volokh, "The mechanisms of the slippery slope" *Harvard Law Review*, 2003, vol. 116, no 4, p. 1026-1137.

35. Antonio Gramsci, *Cahiers de prison* , Gallimard, Tome 3, p. 283

RÉSUMÉS

Dans un arrêt du 17 décembre 2016, la Cour de Luxembourg a invalidé les législations suédoises et anglaises prévoyant une collecte indifférenciée et massive de données d'usagers de télécommunications. La Cour con-firme ainsi la pleine applicabilité aux législations nationales de la condamnation de la surveillance de masse opérée par les arrêts Digital Rights Ireland et Schrems. Plus intéressant, mettant explicitement en œuvre les arrêts Zakharov et Szabo de son homologue strasbourgeoise, la Cour précise pour la première fois en détails les exigences devant présenter une législation relative à la surveillance digitale. Cette confirmation ad libitum de la condamnation de la surveillance électronique de masse élève le niveau de garanties procédurales (trans-parence des traitements et recours effectif) découlant du droit fondamental à la protection des données per-sonnelles consacrée par l'article 8 de la Charte des Droits Fondamentaux de l'Union Européenne. Elle n'est toutefois pas dénuée d'ambiguïtés.

AUTEUR

JEAN-PHILIPPE FOEGLE

) Doctorant en droit public (CREDOF - Université Paris Ouest Nanterre) et allocataire doctoral (Conseil régional d'Ile de France)